2211 North First Street | 95131 San Jose, CA

September 23, 2010

Chairman Julius Genachowski
Federal Communications Commission
445 12th Street, SW
Washington DC 20554

Via electronic filing

RE: Federal Communications Commission
Request for public comments on the creation of a Cybersecurity Roadmap
PS Docket No. 10-146
GN Docket No. 09-51

Dear Chairman Genachowski and Commissioners:

PayPal, a leading global online payment company, is pleased to submit comments in response to the Federal Communication Commission's (FCC) public request for comments on the Commission's creation of a Cybersecurity Roadmap.

PayPal firmly believes that the Internet is an ever more critical resource to the global economy and people's lives, and that preserving an open, innovative, generative Internet is an important goal. We share the FCC's belief that without improvements in the fundamental governance and security of the Internet, it cannot continue to fulfill its promise. It is vital to not conflate principles which would make the Internet as safe as reasonably possible for consumers, with proprietary or commercial interests.

Public policy development in the area of cybersecurity presents its own unique challenges:

1. In the United States there a overlapping areas of responsibility within the various Federal agencies; and
2. As a fully global infrastructure, the policies implemented within the United States must be in alignment with those policies adopted internationally.

In specifically addressing the FCC inquiry, PayPal offers the following guiding principles:

- The success of the Internet ultimately rests upon consumers trusting the Internet and its safety. While this cannot be absolute, it is clear that the current trends are driving the Internet towards less, rather than more, trust.

- Network and telecom regulation should be fully supportive of ecosystem safety and security. Regulations should be narrowly tailored to disallow inappropriate behavior while still allowing network operators and service providers to provide protection against security threats.
- Cybersecurity solutions must require that those best able to provide for security be held responsible and accountable for doing so. In essence, we believe that many of the security and safety problems that the Internet suffers today are due to negative externalities. Using natural choke points to effectively manage negative externalities is one of the most important principles in making the Internet safer.

In creating a Cybersecurity Roadmap, we suggest a discussion structure with five specific areas: end users, infrastructure, web sites and systems, criminal activity, and catastrophic events. This provides a framework for a broad-based discussion of the issues while at the same time encouraging detailed analysis of specific issues.

Internet Service Providers (ISPs) play a central role in the security and governance of the Internet. Because of their role as providers to consumers and business, their backbone transit of both regular Internet traffic and in many cases human-safety critical traffic, and their role in both detecting and responding to large-scale attacks, ISPs must be relied upon to take an active role in making the Internet and the overall communications ecosystem safer.

The FCC should help facilitate ISPs taking an active role in ensuring the security of the ecosystem. The recommendations outlined below encompass the role that ISPs can play in policing malware on the internet and ensuring availability of this critical resource to legitimate traffic while also denying those benefits to criminal activity.

Build a program to stop malware

The network regulator in Australia, the Australian Communications and Media Authority (ACMA), has developed a voluntary program in which:

1. ISPs sign up for the Australian Internet Security Initiative (AISI) program;
2. ACMA uses various intelligence sources to compile a list of Internet Protocol (IP) addresses which are apparently compromised by malware;
3. ACMA communicates that list to the relevant signed up ISPs; and
4. In turn the ISPs then communicate with the end-customer that there's a problem with one or more of their personal computers (PCs).

The program has been in place since about 2007, and has been quite effective. Viewed by the number of ISPs which have signed up, it might not seem very impressive: about 80 out of several hundred. However, the 80 ISPS are the large urban ones, and so AISI now helps protect over 90% of Australian consumers who use the Internet. As such, it's been an extremely effective tool at protecting consumers, as well as a great example of public/private cooperation. Moreover, it's been run on an amazingly small budget and the entire ACMA/AISI team is about half a dozen people.

AISI is an excellent model that should be adopted by all network regulators, such as the FCC. Initially, these programs should be voluntary. However, we also feel strongly that once programs like this have been piloted successfully, they should be made mandatory for all ISPs which offer Internet connection services to consumers and small businesses.

Transit providers are incented, if not mandated, to screen criminal traffic

Most transit providers already have network security programs in place by which they monitor the traffic that passes across their network infrastructure. As such, they frequently know which servers are controlling which botnets, and which PCs have been infected by the botnets. Generally speaking, this can be simply known by looking at the packet headers (i.e. where the network traffic is going from/to), without any inspection of the actual content of the headers. This avoids much of the perception of privacy issues, wherein terms such as "deep packet inspection" are used to imply that security and privacy are at odds with one another.

The transit providers have technical means easily at their disposal to drop this traffic, which is purely criminal in nature. This is an important point: carrying this traffic simply means that criminals hold an advantage, and legitimate Internet users are victimized.

However, as it stands today, the vast majority of Internet backbone transit providers do not interfere with this traffic. The rationale appears to be that there is some uncertainty whether the necessary legal framework exists for them to do so. A reasonable interpretation of the Commission's current policy, and the regulations which Congress have imposed, in fact do give the transit providers the necessary freedom to block this traffic. However, it will be necessary for the FCC to publicly validate this assertion.

It is unclear whether the Commission would be able to force transit providers to take these steps without additional authority from Congress. If the Commission believes that it already has such authority, then we unhesitatingly recommend that it should act to require transit providers to block criminal traffic. If not, then we feel that there is a strong case in requesting the additional authority from Congress to do so.

Ensure hosting providers are incented to properly manage servers

There are two basic challenges with hosting providers:

1. It appears a very small number of providers deliberately target the criminal community as their customer base, and have advertized "bulletproof hosting" schemes; and
2. For the remainder, their quality standards are variable as to how well they secure their servers, and how effective their processes are at dealing with reported problems. One significant complication in

devising a regulatory framework for managing cybersecurity is that there are a number of US agencies which could play a legitimate role and become involved.

While the "bulletproof hosting" problem is relatively small, at least in the United States, it has been extremely frustrating for those tracking cybercrime cases to see such providers operate with apparent impunity. In recent months, action has been taken both by the private sector (which has arranged for such hosting providers to be depeered by their upstream transit providers), and most recently by the FTC. Private industry and security industry specialists should not take on such cases unilaterally, but rather work in tandem with the efforts of the United States government. There needs to be clear delineation of responsibilities in cases such as these to take swift and effective action against criminally motivated hosting providers.

The problem of security standards within the hosting provider space is likely one where the Commission in fact could have good influence, and is reasonably within its remit. There are two sets of standards which need to be considered. First, there needs to be some set of guidelines for hosting providers which lay out the kinds of preventative security measures that hosting providers could reasonably attempt. To be clear, we don't necessarily support making such guidelines mandatory, because information security is a topic where there are frequently multiple approaches to achieving some particular end. However, it is reasonable to lay out some minimum sets of expectations, much in the way that the Payment Card Industry (PCI) standard has done for businesses which process credit cards.

Second, there should be clear expectations of responses from hosting providers, to legitimate requests, either to remove spoof/phishing sites, or to clean up machines that are serving malware, or hosting other malicious activity. It's been PayPal's experience working with the global community of hosting providers that there's a very strong correlation between slow response times and criminal abuse. That is, criminals tend to favor hosting providers which are slow and inefficient at dealing with abuses within their hosting infrastructure. Strong guidance from the Commission to hosting providers would substantially help.

Support improvements to routing security

Well known security flaws in the existing routing protocols on the Internet represent a threat to all users of the system. Existing standards bodies and network operators are working hard on replacements and security enhancements, but the FCC can and should use its influence to ensure that the core routing protocols of the internet are fixed to ensure the continued availability of this critical resource.

Collaborate on cybersecurity with a multitude of other federal agencies

Overall governance and responsibility for improving cybersecurity, especially the security of our communications infrastructure is the responsibility of a variety of governance agencies. To the extent that new technical standards are needed in the area of internet security, the FCC in collaboration with NIST and

2211 North First Street | 95131 San Jose, CA

NTIA should lead the charge in representing US government interests with de facto international standards bodies such as the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF), and de jure international standards bodies such as the International Telecommunications Union (ITU).

The FCC and the Federal Trade Commission (FTC) should jointly share responsibility for consumer security. The FCC should be responsible for any and all technical safeguards, requirements, and the actions of networking and hosting providers. The FTC is perhaps better positioned to deal with issues regarding consumer endpoint security including security controls on devices, contractual provisions between consumers and their software and hardware manufacturers.

Summary

The United States must work, in both domestic and international capacities, to assure that the future of the Internet will be secured by a coordinated global public policy effort. While the challenges posed by cybercrime are not yet life-threatening to the Internet, it is evident that the risks are steadily increasing without evidence that either remedial steps or a comprehensive, global plan of action are in place. Implementation of the actionable recommendations presented in this document is critical to securing the future of the Internet.

Thank you for allowing PayPal to share these comments. As the FCC works through this process, we would be pleased to provide any additional information and insight deemed relevant to assisting your work.

Sincerely,

Michael Barrett
Vice President – Information Risk Management
Chief Information Security Officer